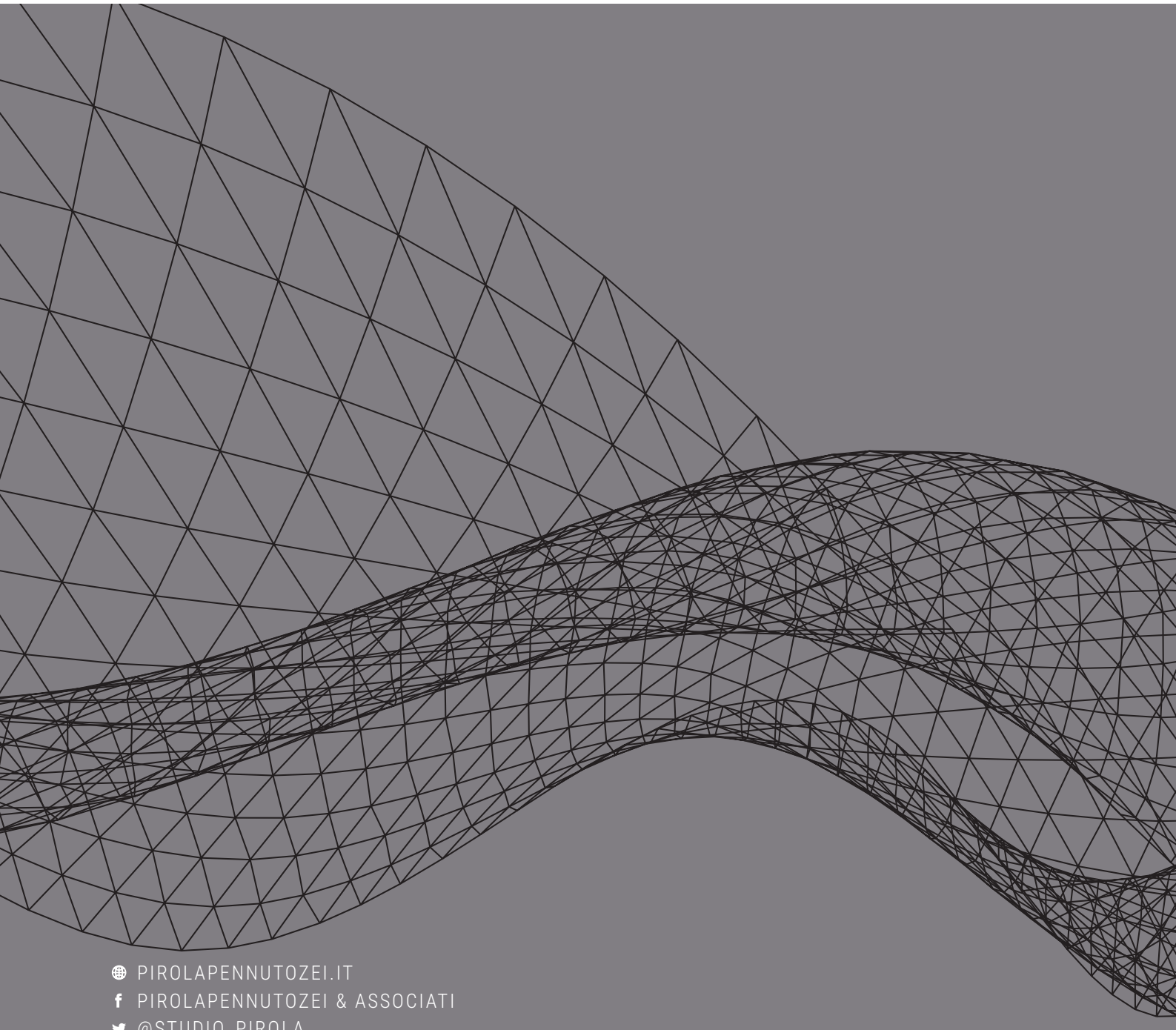
Pirola
Pennuto
Zei
& Associati

studio di consulenza
tributaria e legale

# COMPLIANCE

## NEWSLETTER / MARCH 2018



PIROLAPENNUTOZEI.IT
PIROLAPENNUTOZEI & ASSOCIATI
@STUDIO_PIROLA
PIROLA PENNUTO ZEI & ASSOCIATI

Pirola Pennuto Zei & Associati
studio di consulenza tributaria e legale

INDEX

# LEGISLATION



# GUIDANCE



# COURT DECISIONS



BACK TO TABLE OF CONTENTS ↑

# LEGISLATION

## 1.1
### GDPR, green light by the Council of Ministers

On 21 March last, on conclusion of their preliminary examination, the Council of Ministers approved a draft Legislative Decree enacting article 13 of the Act incorporating European law into Italian legislation 2016-2017 (Act 163 of 25 October 2017), published in the Italian Official Journal on 6 November and entered into force on 21 November.

By this measure the Government has been delegated powers to align domestic rules to the provisions of EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

In exercising the delegation of powers by Parliament, the Council of Ministers abrogated the current Italian Personal Data Protection Code (Legislative Decree no. 196/2003), as expressly required by art. 101 of the newly approved draft decree. The choice is aimed at having a clearer body of personal data protection rules, which at present consists of the directly applicable Regulation and of the draft legislative decree approved on a provisional basis.

We set out below the most significant provisions contained in the draft Legislative Decree approved by the Council of Ministers:

- article 14, "*Assignment of functions and tasks to designated entities*", providing that the Processor and the Controller may delegate tasks and functions to natural persons acting under their authority, thus maintaining the functions assigned to persons within the organization who under the rules previously in force, but in contrast to EU Regulation 2016/679, were named "*persons in charge*";
- articles 88 and 93, governing the manner of sending advertising, direct sales or marketing research or commercial communication material, provisions that, compared with existing regulation, have remained unchanged;
- article 90, governing the "*Storage of traffic data for other purposes*", providing for a storage period of

24 and 12 months for the purposes of ascertaining and prosecuting offences respectively;

- article 97 on the "*Authorizations by the Data Protection Supervisor*", fixing a term of 90 days from the date of entry into force of the draft decree for the evaluation of the adequacy of the current authorizations with relation to the wording of Regulation (EU) 2016/679. The same evaluation will have to be made also in respect of on the measures issued by the Italian data protection authority in the past;
- article 98, named "*Other transitional provisions*", carrying a general interpretation clause, specifying that the reference to Legislative Decree 196/2003 contained in provisions of law or regulations will have to refer to the corresponding provisions of Regulation (EU) 2016/679.

The Legislator has also abrogated some criminal penalties, which may potentially overlap the administrative penalties laid down in Regulation (EU) 2016/679, thus breaching the principle of "*ne bis in idem*" (double jeopardy).

# GUIDANCE

## 2.1

### Safety at work – the ISO 45001: 2018 standard has been published

The approval procedure of the new 2018 ISO 45001 standard on health and safety management systems was completed with its publication on 12 March 2018.

The standard ("*Occupational Health & Safety Management Systems – Requirements with guidance for use*") has the same structure as the environmental management standards (ISO 9001, ISO 14001); however, companies certified under OHSAS 18001: 2007 will have to change their occupational health and safety management systems to adjust to the new ISO standard by March 2021.

## 2.2

### Transparency International: a best practice guide for whistleblowing

Transparency International has published the first Guide for national policy-makers on matters of whistleblowing, providing the best practices to be adopted and the basic principles which should always be complied with, including, first of all, the effective protection of whistleblowers, which is a fundamental aspect for the correct operation of the system.

Whistleblower protection rules are now included in all international treaties: the UN Convention against corruption (articles 8, 13 and 33); the civil law and criminal law conventions of the Council of Europe against corruption (articles 9 and 22 respectively); the Inter-American convention against corruption (article III, par. 8); the Convention of the African Union on preventing and combating corruption (article 5 par. 6); the Arab convention against corruption (article 10 par. 6). These treaties have been implemented by the different national legislations, although there are inevitable differences related to the (substantive and procedural) legal aspects of each legal system.

Despite that, "*to date* – says the Guide - *no whistleblowing law is fully aligned with the 30 Transparency International principles. In fact, all existing national laws on whistleblower protection still have loopholes and shortcomings.*"

As regards Italy, whistleblowing regulations, although very recent, do not comply with a series of very important principles, thus giving rise to criticism. We refer, for instance, to the fact that, in the private companies' sector, the system applies to companies having a "*231*" Model, solely for predicate offences which trigger corporate administrative liability of entities and to "*top managers and persons subjected to direction and surveillance by top management*".

Furthermore, no reward system (principle 23), or reference institutional authority, as is A.N.AC. (Italian anti-bribery authority) for public entities (principle 28) have been introduced for private companies.

## 2.3
### New FAQs issued by the Data Protection Supervisor on the Data Protection Officer (DPO) of private entities

On 15 December 2017 the Data Protection Supervisor published the FAQs regarding the Data Protection Officers (DPOs) of public entities; subsequently, it provided new instructions on the appointment of a DPO by private entities.

The replies to eight of the questions most frequently asked by operators were published On 26 March. The Data Protection Supervisor has therefore confirmed its stance on the matter, including in relation to the principles clarified by the former Article 29 Data Protection Working Party.

The first reply focused on the role of the DPO, who will have functions of support, control, consultancy, training and information with regard to the application of the Regulation, will cooperate with the authority (his/her name must be notified to the Data Protection Supervisor) and will be the contact persons for all parties concerned. This is, therefore, a complex role, with several functions which must necessarily be well-coordinated and well-balanced.

The second reply refers to the requirements to be fulfilled by the DPO. He/she need not be registered with a list or have received specific certifications but must know the law and the guidance, and the rules of the relevant place of work, must act autonomously and independently, without receiving any instructions, and will directly report to top managers; an office and resources will have to be made available to him/her for the performance of his/her tasks.

The third reply refers to the sensitive aspect of whether or not the appointment of a DPO is mandatory: in the Data Protection Supervisor's intentions, a DPO must necessarily be appointed by the entities whose core business consists of carrying out processing which requires regular and systematic large-scale monitoring of data subjects, or large-scale processing of special categories of personal data or data relating to criminal convictions and offences. In this regard, a series of examples are provided with reference to the categories required to appoint a DPO, i.e. banks, insurance companies, credit information systems, financial companies, commercial information companies, auditing companies, debt recovery companies, security service companies, political parties and movements, trade unions, tax assistance offices, *patronati* (charitable institutions), utility (telecommunications, electricity or gas) companies, staff supply and recruitment firms, companies engaged in the health and prevention sector, such as private hospitals, spas, medical analysis laboratories and rehabilitation centres, call centres, companies providing IT services and pay TV providers.

On the contrary, as regards the entities not required to appoint a DPO, the FAQs refer to processing carried out by self-employed professionals operating on an individual basis in respect of agents, representatives and mediators operating not on a large scale, sole proprietors or family businesses, small- and medium-sized firms for the processing of personal details related to the recurring management of the relationships with suppliers and employees.

However, it is recommended, for accountability purposes, to appoint a DPO including when the Controller or Processor are not required to, in order to guarantee greater security.

In the fifth reply, it is specified that entrepreneurial groups can appoint a single DPO, provided that he/she can easily be contacted by each factory, can communicate with the persons involved in an effective manner and, above all, can cooperate with the supervisory authorities.

The position of DPO can be held by an employee of the controller or processor, provided that there is no conflict of interests, who knows the environment where processing is carried out. At the same time, this position can be held by external persons, provided that they guarantee the actual performance of the tasks established by the Regulations. Whether an "*internal*" or "*external*" DPO is appointed can be freely decided by the Controller or the Processor.

"*Internal*" Data Protection Officers must be appointed by a specific deed, while "*external*" data protection officers, who will have the same characteristics and protections as internal DPOs, will be designated by a service agreement. Such deedsof appointment must be drawn up in writing, must expressly include the tasks assigned, the resources necessary for the performance of the duties, as well as any other relevant information.

Both internal and external DPOs will operate with adequate support consisting of financial resources, facilities and, if necessary, staff. The Controller or the Processor who have appointed a DPO are however fully responsible for his/her compliance with the law on data protection and must be able to demonstrate such compliance. The appointment of a DPO does not relieve the Data controller from responsibility regarding the processing of data, which lies with the company's senior management.

In the seventh reply it is explained that the position of a DPO is compatible with the assignment of other tasks, provided that there is no conflict of interests. In this regard, it is preferable to avoid the appointment of members of the senior management (managing director, a member of the board of directors, general manager, etc.), or of departments with decision-making powers regarding the purposes and procedures of processing (HR, marketing, financial, IT divisions etc.). In the absence of a conflict of interests and depending on the context, the appointment of the heads of staff support functions (e.g. head of legal affairs) should be carefully evaluated.

Finally, as regards the appointment of an "*individual*" or a "*legal entity*", it has been clarified that the Regulation expressly prescribes that the DPO may also be an "*employee*" of the Controller or Processor and that, if an "*external*" DPO is chosen, a legal entity may be appointed.

## 2.4
### The Data Protection Supervisor prohibits spamming of the certified email accounts of self-employed professionals

The Data Protection Supervisor has prohibited companies or related associations from sending unsolicited promotional email messages to the certified email accounts of self-employed professionals.

Verifications had shown that the voluntary staff of an association and a third-party company had gathered

the certified email addresses of lawyers, tax consultants, auditors, labour consultants and notaries public, thus violating the fundamental principles of lawfulness, fairness and purpose of data processing.

The company had sent to more than 800,000 professionals email messages announcing the publication of a call for tenders for "*reputational consultants*", an invitation to a webinar and articles on the sending company.

In addition to being processed without consent, the certified email addresses had been unlawfully collected from INI-PEC (the Italian registry of web addresses), from the Companies' registry website (*www.registroimprese.it*) and from the lists of professionals published by some local associations. The law stipulates that the extraction of certified email addresses from the companies' registry or professional lists "*is allowed solely to public authorities for the service of notices in connection with administrative requirements*". In one case email messages had been sent even after that the recipient had formally objected to the processing of his/her personal data, by exercising the rights prescribed by the Personal Data Protection Code.

The explanations provided by the company and the association were of no avail. Among other things, they considered themselves exempted from the obligation to request preliminary consent based on the "*institutional*" nature of notifications. As clarified by the Data Protection Authority, the email messages promoted the association's activities in relation to a "*reputational consultant*" and accordingly should have been sent in compliance with the provisions of the Personal Data Protection Code and the Data Protection Supervisor's Guidelines on promotional activities and the prohibition of spamming. The Data Protection Authority has consequently prohibited the company and the association from unlawfully processing the professionals' data and ordered their cancellation, and has reserved the possibility to consider charging a penalty.

## 2.5

### Prohibition of massive control and unlimited conservation of email messages

The Personal Data Protection Authority has prohibited a company from processing its employees' business-related email messages in violation of the regulations on data protection and labour laws.

The Authority ascertained that the company had unlawfully processed the personal data included in incoming and outgoing email messages, including private messages, exchanged by an employee with his colleagues and associates. The data collected during a two-year period had then been utilized as basis for a disciplinary action followed by the employee's dismissal, which had been subsequently annulled by the labour judge.

The Authority stated that the company had not provided the employees with information on the procedures and purposes of the collection and storage of data, either in individual privacy notices or in the company's policy, in evident contrast with the company's obligation to inform the staff on the key characteristics of processing. The company also kept external data and the contents of all email messages exchanged by the employees not only for the entire term of their employment, but also thereafter, in violation of the principles of fairness, necessity and proportionality set out by the Data Protection Code.

According to the Data Protection Supervisor, the company should not have carried out such invasive processing, but should have introduced document management systems able to identify the documents to be stored. The failure to comply with the above mentioned principles, resulting in the extended and systematic storage of email messages for an indefinite term, as well as the possibility for the employer to use them for unclear and indefinite purposes, "*…gave the employer control over the employees' activity. Such control is prohibited by the relevant regulations which do not allow massive, prolonged and indiscriminate verifications. Although the employer can check the correct performance of a task and the proper use of work instruments, it must always safeguard the freedom and dignity of employees.*"

Finally, the Data Protection Supervisor stated that accessing the employee's incoming business emails after his dismissal was not compliant with the principle of reasonable expectation of privacy of correspondence. At the end of an employment relationship, the terminated employee's email account must necessarily be deactivated and removed, and replaced by other accounts.

# COURT DECISIONS

## 3.1

**Whistleblowing: anonymity only means non-disclosure a person's identity**

By decision no. 9047/2018 the Court of Cassation has pronounced on whistleblowing for the first time after the publication of Act no. 179/2017. The decision refers to the sphere of public companies but offers useful indications for the private sector as well.

In the case at issue, the Court of Cassation rejected the appeal filed by an employee of the Revenue Agency under investigation for severe fraud, fraudulent misrepresentation in e-documents and corruption for actions contrary to official duties, and confirmed the accusations triggered by an anonymous report submitted by a colleague.

The employee's objection that the report could not be used because it was unsigned, was of no avail. He claimed in particular the non-enforceability of the judge's order against him based on the whistleblower's report, since no official witness statement in accordance with art. 203(1) of the Italian code of criminal procedure had been given.

Conversely, the Court of Cassation pointed out that the report was fully usable because its author had been identified, although he was treated as an anonymous witness by the judge for preliminary investigations. The whistleblowing channel provided for by art. 54-*bis* of Legislative Decree 165/2001 (Consolidated Legislation on Employment in the Public Sector) ensures non-disclosure of the whistleblower's identity, in the sense that the employee who uses an internal email account to report a wrongdoing does not need to sign the document but can be identified through his/her credentials, although his identity is protected.

Furthermore, the whistleblower had not maintained anonymity during the criminal proceedings and could not thus be classified as an informant, whose statements can be used only if issued as part of criminal proceedings.

Therefore, the court confirmed the measures against the employee due to severe circumstantial evidence of his guilt based on a whistleblower's report.

## 3.2

**The notion of non-seriousness of the offence is not extended to bodies corporate**

By decision no. 9072/2018, the Court of Cassation clarified whether corporate liability pursuant to Legislative Decree 231/2001 arises when the offence is acknowledged to be of a non-serious nature. The matter is not expressly regulated by the legislation.

According to the Court of Cassation the body corporate must be judged both under the principle of autonomy of the body corporate's liability laid down in article 8 of the Decree and in the light of the nature of the offence.

The Court of Cassation stated that the lower court's ruling "*affirms that although there is no conviction, corporate liability does arise and therefore the decision cannot be regarded as an acquittal, as the offence continues to exist, both historically and legally*".

Therefore, with regard to corporate liability pursuant to Legislative Decree "*231*", "*in case of a court decision which takes into account the mitigating circumstances of the non-seriousness of an offence for the natural person who perpetrated the offence, the judge must separately ascertain the corporate liability of the legal persons in whose interest and to whose advantage the offence was perpetrated*".

Pirola
Pennuto
Zei
& Associati
studio di consulenza
tributaria e legale

Via Vittor Pisani, 20
20124 Milano

T. +39.02.669951
F. +39.02.6691800

info@studiopirola.com
www.pirolapennutozei.it

# COMPLIANCE NEWSLETTER | MARCH 2018

LEGISLATION, MINISTERIAL GUIDANCE AND CASE LAW AT 31 MARCH 2018.
THIS NEWSLETTER IS INTENDED AS A SUMMARY OF KEY DEVELOPMENTS AND HIGHLIGHTS MATTERS OF GENERAL INTEREST, AND THEREFORE SHOULD NOT BE USED AS A BASIS FOR DECISION-MAKING.
FOR FURTHER DETAILS AND INFORMATION, PLEASE CONTACT YOUR RELATED PARTNER OR SEND AN EMAIL TO UFFICIOSTUDI@STUDIOPIROLA.COM